BAB 1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi telah memberikan dampak signifikan bagi berbagai sektor, termasuk pelayanan kesehatan. Menurut Kementerian Kesehatan RI tahun 2020, Rumah Sakit adalah institusi pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan perorangan secara paripurna yang menyediakan pelayanan rawat inap, rawat jalan, dan gawat darurat (Kemenkes RI, 2020). Rumah sakit sebagai institusi pelayanan kesehatan dituntut untuk menghadirkan layanan yang efektif, efisien, dan tepat waktu melalui pemanfaatan sistem informasi. Salah satu implementasi teknologi informasi dalam layanan kesehatan adalah penggunaan Sistem Informasi Manajemen Rumah Sakit (SIMRS), yang mendukung proses pelayanan serta pengelolaan informasi secara terintegrasi.

Salah satu komponen penting dalam SIMRS adalah Rekam Medis Elektronik (RME). Menurut Permenkes Nomor 24 tahun 2022 rekam medis elektronik adalah rekam medis yang dibuat dengan menggunakan sistem elektronik yang diperuntukkan bagi penyelenggaraan rekam medis. Penyelenggaraan rekam medis elektronik digunakan untuk pencatatan data medis pasien secara digital, aman, dan mudah diakses oleh petugas kesehatan yang berwenang. Pemanfaatan RME diharapkan dapat meningkatkan akurasi diagnosa, kontinuitas pelayanan, serta kualitas pengambilan keputusan klinis.

Namun, penerapan teknologi informasi dalam bidang kesehatan juga menimbulkan tantangan, khususnya terkait keamanan data. Informasi kesehatan merupakan data yang bersifat sensitif dan memiliki tingkat kerahasiaan tinggi, sehingga berpotensi menjadi target serangan siber. Kasus kebocoran data pasien yang terjadi di Indonesia dalam beberapa tahun terakhir menunjukkan bahwa risiko tersebut tidak dapat diabaikan. Pada tahun 2021 terjadi kebocoran data BPJS Kesehatan yang memengaruhi sekitar 279 juta penduduk, dan pada tahun 2022 kembali ditemukan dugaan kebocoran 6 juta data pasien beserta dokumen rekam medis dengan ukuran mencapai 720 GB. Kondisi ini menjadi indikator nyata bahwa

keamanan informasi kesehatan merupakan aspek kritis yang harus dijaga. (tambah sumber)

Keamanan informasi dalam RME mencakup perlindungan data dari akses ilegal, perubahan yang tidak sah, serta gangguan yang dapat menyebabkan data tidak dapat digunakan. Dicantumkan dalam Permenkes No. 24 Tahun 2022, terdapat 3 pasal yang menjelaskan keamanan rekam medis elektronik ialah dari pasal 29 hingga pasal 31. Pasal 29 menegaskan prinsip-prinsip utama yang harus diikuti dalam penyelenggaraan rekam medis elektronik (RME) untuk memastikan keamanan dan perlindungan data, ialah terdapat 3 hal diantaranya kerahasiaan dan informasi RME, integritas, dan ketersediaan RME dapat diakses oleh individu. Pasal 30 memberikan penjelasan lebih lanjut mengenai hak akses yang diberikan kepada tenaga kesehatan dalam mengelola data RME, termasuk penginputan data, perbaikan data, dan melihat data untuk keperluan pelayanan atau administrasi (Wardani et al., 2024).

Rumah Sakit Pusat Angkatan Darat Gatot Soebroto merupakan rumah sakit tipe A yang berlokasi di Jakarta Pusat. RSPAD Gatot Soebroto Puskesad merupakan rumah sakit rujukan tertinggi bagi Rumah Sakit TNI di seluruh Indonesia. RSPAD Gatot Soebroto Puskesad telah mengimplementasikan rekam medis elektronik yang telah terintegrasi dengan SIMRS RSPAD sejak bulan September 2023. Sebagai rumah sakit yang telah mengadopsi RME, Penerapan RME menuntut pengelolaan keamanan informasi yang lebih optimal agar pelayanan kesehatan dapat berjalan tanpa hambatan dan data pasien tetap terlindungi.

Berdasarkan hasil observasi dan wawancara selama pelaksanaan Praktik Kerja Lapangan (PKL) di RSPAD Gatot Soebroto Puskesad, ditemukan beberapa permasalahan terkait keamanan informasi pada Sistem Informasi Manajemen Rumah Sakit (SIMRS). Aspek kerahasiaan (Confidentiality) merupakan prinsip fundamental dalam keamanan informasi yang bertujuan untuk menjaga agar data hanya dapat diakses oleh pihak-pihak yang memiliki otorisasi. Dalam konteks ini, masih terdapat kelemahan pada mekanisme autentikasi, di mana sebagian petugas belum melaksanakan penggantian kata sandi secara berkala. Selain itu, sistem belum menerapkan kebijakan kata sandi yang kuat, seperti kewajiban penggunaan

karakter khusus atau kombinasi huruf dan angka, sehingga berpotensi menurunkan tingkat keamanan kredensial pengguna. Tidak adanya pembatasan jumlah percobaan login juga menambah kerentanan sistem terhadap serangan *brute force*. Oleh karena itu, kondisi tersebut mengindikasikan bahwa upaya perlindungan terhadap kerahasiaan data pengguna belum sepenuhnya memenuhi prinsip keamanan informasi yang ideal. Aspek ketersediaan (*Availability*) merupakan komponen penting dalam keamanan informasi yang memastikan agar data dan sistem informasi dapat diakses serta digunakan oleh pihak yang berwenang kapan pun dibutuhkan. Namun, penempatan server utama dan server cadangan yang berada dalam satu gedung menimbulkan risiko yang signifikan terhadap keberlangsungan operasional sistem. Kondisi ini menyebabkan kedua server memiliki kerentanan yang sama terhadap insiden fisik, seperti kebakaran, gangguan listrik, maupun bencana alam. Apabila terjadi insiden tersebut, sistem berpotensi tidak dapat diakses pada saat kritis, yang dapat menghambat proses pelayanan dan operasional. Oleh karena itu, konfigurasi infrastruktur yang tidak memperhatikan prinsip redundansi lokasi menunjukkan bahwa aspek ketersediaan dalam sistem belum sepenuhnya diterapkan secara efektif.

Maka dari itu dibutuhkan penelitian mendalam menggunakan metode CIA. Metode CIA merupakan terminologi dalam bidang keamanan yang diartikan sebagai tujuan keamanan yang memerhatikan pada kerahasiaan (Confidentiality), integritas (Integrity), dan ketersediaan (Availability) data. Dengan menggunakan CIA, upaya pengamanan siber sistem menjadi lebih efektif dan terstruktur, sehingga membuktikan bahwa CIA adalah kerangka kerja untuk strategi keamanan siber yang mampu diterapkan pada berbagai organisasi (Farkhan Nindyarayhan Dhanendra, 2024). Model ini menekankan tiga pilar utama keamanan, yaitu menjaga kerahasiaan data dari akses yang tidak berwenang (confidentiality), menjamin keakuratan dan keutuhan informasi dari tindakan manipulasi atau perubahan ilegal (integrity), serta memastikan bahwa data dan sistem selalu tersedia bagi pihak yang berwenang ketika diperlukan (availability). Pendekatan ini sejalan dengan ketentuan keamanan data pada Rekam Medis Elektronik yang telah diatur dalam Permenkes Nomor 24 Tahun 2022 serta standar internasional ISO/IEC

27001:2013 sehingga hasil penelitian diharapkan dapat memberikan rekomendasi perbaikan keamanan yang efektif dan sesuai standar.

Oleh karena itu, penulis tertarik untuk melakukan penelitian dengan judul "Tinjauan Keamanan Informasi Data pada SIMRS RSPAD Gatot Soebroto Puskesad Berdasarkan Aspek Confidentiality, Integrity, dan Availability (CIA)" sebagai upaya untuk mengevaluasi tingkat keamanan informasi rekam medis elektronik serta memberikan rekomendasi perbaikan sesuai standar keamanan data yang berlaku

1.2 Tujuan dan Manfaat

1.2.1 Tujuan Umum PKL

Meninjau keamanan informasi dan rekam medis elektronik di SIMRS RSPAD Gatot Soebroto Puskesad.

1.2.2 Tujuan Khusus PKL

a. Meninjau aspek kerahasiaan (*Confidentiality*) pada pengelolaan data rekam medis elektronik di SIMRS RSPAD Gatot Soebroto Puskesad, khususnya dalam mekanisme login, dan perlindungan terhadap kebocoran informasi pasien.
b. Meninjau aspek keutuhan data (*Integrity*) pada sistem informasi manajemen rumah sakit (SIMRS) RSPAD Gatot Soebroto Puskesad untuk memastikan bahwa data rekam medis elektronik tidak mengalami perubahan tanpa otorisasi dan tetap akurat serta konsisten selama penyimpanan maupun transmisi.
c. Meninjau aspek ketersediaan (*Availability*) pada sistem informasi rekam medis elektronik di RSPAD Gatot Soebroto Puskesad guna mengetahui sejauh mana sistem mampu menjamin ketersediaan data bagi pengguna yang berwenang saat dibutuhkan, termasuk upaya pemulihan data saat terjadi gangguan sistem dan *recovery* bencana.

1.2.3 Manfaat PKL

a. Bagi Rumah Sakit

Sebagai bahan masukan dan pertimbangan bagi rumah sakit untuk rekomendasi peningkatan fitur keamanan di RSPAD Gatot Soebroto Puskesad guna menjaga informasi data privacy dan data security rekam medis elektronik.

b. Bagi Mahasiswa

Sebagai wujud dari penerapan ilmu pengetahuan yang selama ini telah diperoleh selama masa perkuliahan terutama dalam memberikan gambaran terkait keamanan data pada implementasi rekam medis elektronik di RSPAD Gatot Soebroto Puskesad.

c. Bagi Politeknik Negeri Jember

Sebagai bahan referensi bagi penelitian selanjutnya khususnya pada bidang keamanan data rekam medis elektronik serta pengembangan ilmu pengetahuan di Politeknik Negeri Jember.

1.3 Lokasi dan Waktu

1.3.1 Lokasi

Penelitian ini dilaksanakan di Rumah Sakit Pusat Angkatan Darat Gatot Soebroto. Penelitian khususnya dilakukan pada Insatalasi Rekam Medis dan Infokes, Infolahta. Penelitian ini dilakukan selama masa Praktik Kerja Lapang (PKL).

1.3.2 Waktu

Kegiatan praktik kerja lapang ini dilaksanakan pada tanggal 25 Agustus sampai 14 November 2025, praktik kerja lapang ini dilakukan setiap hari Senin hingga hari Jumat, dan pada hari Sabtu ada 2 mahasiswa yang bertugas jaga di pendaftaran IGD.

1.4 Metode Pelaksanaan

1.4.1 Jenis Penelitian

Jenis penelitian yang digunakan dalam tinjauan keamanan informasi pada Sistem Informasi Manajemen Rumah Sakit (SIMRS) RSPAD Gatot Soebroto Puskesad adalah penelitian kualitatif. Penelitian ini bertujuan untuk menggali secara mendalam penerapan kebijakan dan prosedur keamanan informasi pada sistem, khususnya terkait dengan aspek kerahasiaan (confidentiality), keutuhan data (integrity), ketersediaan informasi (availability). Pendekatan ini digunakan untuk memperoleh gambaran yang komprehensif mengenai sejauh mana sistem telah menerapkan prinsip-prinsip keamanan informasi sesuai dengan standar dan kebijakan yang berlaku di lingkungan RSPAD Gatot Soebroto Puskesad.

1.4.2 Subjek dan Objek Penelitian

Subjek dari penelitian ini adalah pengguna SIMRS oleh PPA pengisi rekam medis elektronik yakni perawat, petugas rekam medis (pelayanan data, pendaftaran, pelaporan), petugas Infolahta (pengelola SIMRS). Objek penelitian dari penelitian ini adalah SIMRS RSPAD Gatot Soebroto Puskesad bagian rekam medis elektronik di RSPAD Gatot Soebroto Puskesad.

1.4.3 Sumber Data

Data yang digunakan dalam penelitian ini adalah data primer dan data sekunder:

a. Data primer adalah sumber informasi utama yang dikumpulkan secara langsung oleh peneliti dalam proses penelitian. Data ini diperoleh dari sumber asli, yaitu responden atau informan yang terkait dengan variabel penelitian. Data primer dapat berupa hasil observasi, wawancara, atau pengumpulan data melalui angket (Rukhmana, 2021).
b. Data sekunder adalah sumber data penelitian yang diperoleh secara tidak langsung melalui media perantara. Artinya, data ini tidak dikumpulkan langsung oleh peneliti melainkan dari sumber yang telah ada sebelumnya, seperti dokumen, literatur, atau data yang dikumpulkan oleh pihak lain (Rukhmana, 2021).

1.4.5 Teknik Pengumpulan Data

a. Observasi adalah suatu proses yang kompleks yang terdiri dari berbagai proses biologis dan psikologis yang melibatkan pengamatan, persepsi, dan ingatan. Observasi ini dilakukan dengan mengamati fitur keamanan pada rekam medis elektronik di SIMRS RSPAD Gatot Soebroto Puskesad.
b. Wawancara merupakan pertemuan dua orang untuk bertukar informasi dan ide melalui tanya jawab, sehingga dapat dikonstruksi makna dalam suatu terntentu Dalam penelitian ini peneliti melakukan wawancara kepada pengguna SIMRS.
c. Dokumentasi adalah suatu cara untuk memperoleh data dan informasi dalam bentuk buku, arsip, dokumen, tulisan angka, dan sebagainya. Dokumentasi yang dilakukan dalam penelitian ini adalah hasil foto atau rekaman pada saat penelitian di RSPAD Gatot Soebroto Puskesad.